PRIVACY TRAINING 101

What you Need to Know about Safeguarding Protected Personal Information and Personally Identifiable Information (PPI/PII)

DEFINITIONS

- “PPI” stands for Protected Personal Information
- “PII” stands for Personally Identifiable Information
- PPI and PII are interchangeable
- PPI/PII is: Information which can be used to identify a person uniquely and reliably, including but not limited to name, SSN, address, telephone #, e-mail address, mother’s maiden name

Purpose of this training:

- To focus on the importance of PRIVACY and to ensure all OSD/JS personnel (military, civilian, contractor) are aware of the vital role that they must play in ensuring that PPI/PII is properly protected from unauthorized disclosure.

Why You Need to Know About Privacy:

- We are collection, maintaining, distributing and disposing of information about individuals--YOU!
- The law requires you to take precautions when collecting, maintaining, distributing and disposing of PPI/PII
- The Privacy Act of 1974 contains both civil and criminal penalties for non-compliance.

The Department of Veterans Affairs Breach

- The VA loss of thousands of veterans' records was well publicized, costly and brought PRIVACY to the forefront.
- This breach resulted in Presidential and Congressional interest in PRIVACY
- Office of Management & Budget ("OMB") established working groups to address better protections, notification protocols, costs, and actions to be taken against employees

The Fallout

- OMB issued a Memorandum dated May 22, 2006, entitled “Safeguarding Personally Identifiable Information,” which directed agencies to provide training to all employees on their responsibilities to safeguard personally identifying information

The Fallout (Cont'd)

- OMB issued another Memorandum dated May 22, 2007, entitled "Safeguarding Against and Responding to the Breach of Personally Identifying Information"
- Both Memoranda require agencies to provide PRIVACY training to all employees

Your Role in PRIVACY

- You must understand the importance of ensuring that PPI/PII is properly protected
- You must get involved in identifying best practices for protecting PPI/PII
- You must be aware of the consequences for non-compliance

Privacy Act Requirements

- Establish rules of conduct for collecting, maintaining, distributing, and disposing of personal information
- Publish Privacy Act system of records notices in the *Federal Register* for all approved collections of privacy information
- Ensure that we collect only data that is authorized by law & that we share information only with those who have a need-to-know

Privacy Act Requirements

- Establish and apply data safeguards to protect information from unauthorized disclosure
- Allow individuals to review records about themselves for completeness and accuracy & to amend any factual information that is in error
- Keep record of disclosures made outside of DoD to authorized “routine users” described in the system notice

Examples of Personal Data Requiring Protection

- Financial, credit and medical data
- Security clearance level
- Leave balances; types of leave used
- Home address & telephone numbers, personal e-mail address
- Social Security Number
- Mother’s maiden name; other names used

Examples of Personal Data Requiring Protection

- Drug test results & fact of participation in rehabilitation program
- Family data
- Religion, race, national origin
- Performance ratings
- Names of employees who hold government-issued travel cards

The Loss of PPI/PII

- Can be embarrassing & cause emotional distress.
- Can lead to identity theft, which is costly to the individual and to the Government
- Can impact our business practices & result in actions being taken against an employee
- Can erode confidence in the Government's ability to protect information

DepSecDef Memorandum

- On June 15, 2005, the DepSecDef issued a Memorandum entitled, “Notifying Individuals When Personal Information is Lost, Stolen, or Compromised.”
  - Requires DoD activities to notify individuals within 10 days after the loss or compromise of protected personal information is discovered

DepSecDef Memorandum

- Directs that notification advise individuals of:
- (1) what specific data was involved;
- (2) the circumstances surrounding the loss, theft, or compromise;
- (3) what protective steps the individual can take in response
- See also 32 C.F.R. § 310.50

Additional Breach Notification Procedures

- Agencies must report all incidents involving PII to the U.S.-Computer Emergency Response Team (“US-CERT”) within ONE HOUR of discovery--32 C.F.R. § 310.50(1).
- DoD Components must report all incidents involving PII to the Senior Component Official for Privacy within 24 hours of discovering the breach--32 C.F.R. § 310.50.

Additional Breach Notification Procedures

- Senior Component Official for Privacy, or a designee, shall notify the Defense Privacy Office of the breach within 48 hours upon being notified of the breach--32 C.F.R. § 310.50(2).
- Submit report to the Defense Privacy Office detailing the specifics of the breach--32 C.F.R. § 310.50(2)(i) - (iv).

Collecting PPI/PII

- If you collect it--you must protect it!
- If in doubt, leave it out! Do you really need the entire SSN or will the last 4 digits serve as a second qualifying identifier?
- Moving from a paper process to an electronic process requires you to identify any breach risks

Think PRIVACY When Safeguarding PII

- Need to address whether collection and maintenance of all the information that we collect is "relevant and necessary," and whether we can maintain "timely and accurate" information.
- The CIO may need to conduct a Privacy Impact Assessment ("PIA") of electronic system to identify vulnerabilities.

Best Practices

- Think PRIVACY when considering the PII that you store on your computer, memory stick, PDA, etc.
- Think PRIVACY when you send/receive e-mails that contain PII--are these messages properly marked?
- “FOR OFFICIAL USE ONLY-PRIVACY SENSITIVE-Any misuse or unauthorized access may result in both civil and criminal penalties.”

Best Practices

- Any email messages that contain PII/PPI must contain the proper markings AND be ENCRYPTED!
- Any PII/PPI that is contained or maintained on “mobile” equipment (PDAs, memory sticks etc.) must be ENCRYPTED!

Best Practices

- Think PRIVACY when you create documents--do you need to include the entire SSN?
- Think PRIVACY when placing documents in public folders in Outlook and on public web sites.
- Think PRIVACY when disposing of PII--use cross-cut shredding, if possible

Your Responsibilities

- Do NOT collect personal data without authorization.
- Do NOT distribute or release personal information to other employees unless they have an official need-to-know.
- Do NOT be afraid to challenge anyone who asks to see PA information.
- Do NOT maintain records longer than permitted.

Your Responsibilities

- Do NOT destroy records before disposal requirements are met.
- Do NOT place unauthorized documents in PA systems of records.
- Do NOT commingle information about different individuals in the same file.
- Do NOT transmit personal data without ensuring that it is properly marked.

Your Responsibilities

- Do NOT use interoffice envelopes to mail Privacy data.
- Do NOT place privacy data on shared drives, multi-access calendars, the Intra or Internet that can be accessed by individuals who do not have an official need-to-know.
- Do NOT hesitate to offer recommendations on how to better manage Privacy data.

Privacy Resources

- The Defense Privacy Office website--www.defenselink.mil/privacy.
- The Department of the Navy's Privacy website-www.privacy.navy.mil.
- Department of Homeland Security's Privacy Office website--www.dhs.gov.
- The DOD CIO website--www.defenselink.mil/cio-nii